PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-324972
(43)Date of publication of application : 25.11.1994

(51)Int.Cl. G06F 13/00
G06F 1/00
H04L 12/28

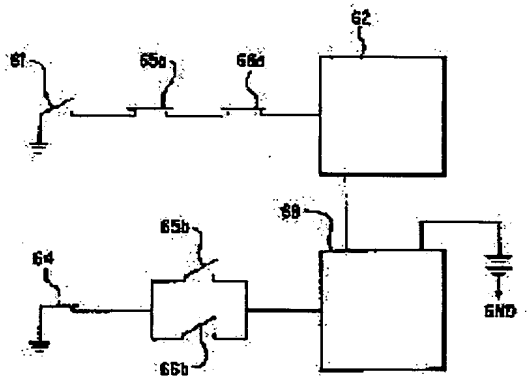
(21)Application number : 05-202015
(22)Date of filing : 23.07.1993

(71)Applicant : INTERNATL BUSINESS MACH CORP <IBM>
(72)Inventor : DAYAN RICHARD A
LE KIMTHANH D
MITTELSTEDT MATTHEW T
NEWMAN PALMER E
RANDALL DAVE L
RUOTOLO LISA A
YODER JOANNA B

(30)Priority
Priority number : 92 947019 Priority date : 17.09.1992 Priority country : US

(54) LAN STATION PERSONAL COMPUTER AND SECURITY PROTECTION METHOD

(57)Abstract:
PURPOSE: To provide a LAN station personal computer and a security protection method.
CONSTITUTION: In a method for protecting a system from an attack on a network to which a LAN station belongs and whose security is protected and in a medialess personal computer system work station (defined as LAN station here), a flag bit showing whether access to the specified security protection mechanism of the system is possible or not during a power on self test is set in a memory in the system, a procedure for obtaining a program for system constitution setting, which is stored in the network, is shown for guiding, a changing and eliminating a password used in the LAN station and password data is prevented from being transmitted on the network.



LEGAL STATUS

[Date of request for examination]	23.07.1993
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	2075806
[Date of registration]	25.07.1996
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	18.12.1998

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平6－324972

(43)公開日　平成６年(1994)11月25日

(51)Int.Cl.⁵	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　13/00	３５４　Ｚ	7368－5Ｂ		
1/00	３７０　Ｅ			
Ｈ０４Ｌ　12/28				
		8732－5Ｋ	Ｈ０４Ｌ　11/00	３１０　Ｚ

審査請求　有　請求項の数３　ＦＤ　（全 19 頁）

(21)出願番号　特願平5－202015

(22)出願日　平成５年(1993)７月23日

(31)優先権主張番号　０７／９４７，０１９

(32)優先日　1992年９月17日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(72)発明者　リチャード・エイ・ダイヤン
アメリカ合衆国　33487　フロリダ州・ボカラトン73ストリート　830　エヌ・イー

(74)代理人　弁理士　合田　潔　（外２名）

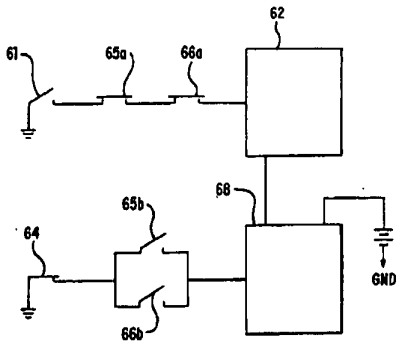
最終頁に続く

(54)【発明の名称】　ＬＡＮステーション・パーソナル・コンピュータ及び機密保護方法

(57)【要約】

【目的】ＬＡＮステーション・パーソナル・コンピュータ及び機密保護方法を提供する。

【構成】ＬＡＮステーションが属し、機密保護を施されたネットワークに対する攻撃がらシステムを保護する方法と、メデイアレス・パーソナル・コンピュータ・システム・ワークステーション（ここではＬＡＮステーションと定義されている）で、パワーオン・セルフテスト中に、システムの特定の機密保護機構へのアクセスが可能であるかどうかを示すフラグ・ビットがシステム内のメモリにセットされ、ネットワークに記憶されたシステム構成設定用プログラムを、該ＬＡＮステーションで使用するパスワードの導入、変更、削除の為、取得する手順を示し、パスワード・データをネットワーク上に送出する事を回避する。



【特許請求の範囲】

【請求項１】　ネットワークとデータを交換し、システムにアクセス可能なデータを不正なアクセスから保護する能力を有するＬＡＮステーション・パーソナル・コンピュータ・システムであって、

コマンドを入力するためのユーザ入力装置と、

通常閉じているカバーと、

カバー錠の鍵の所有者以外のカバー内部へのアクセスを拒絶するため、上記のカバーを機密保護状態に維持するためのカバー錠と、

パスワード・データを受取り、記憶し、選択して動作可及び動作不可の状態にできるように上記のカバー内に取り付けられた消去可能なメモリ要素と、

上記のカバーの内部に取り付けられ、カバーの中からのみアクセス可能で、上記の消去可能メモリ要素を動作可及び動作不可状態にセットするために上記の消去可能メモリ要素に接続して動作するオプション・スイッチと、

上記のカバー内に取り付けられ、上記のメモリ要素の動作可及び動作不可状態を区別することにより、システムにアクセス可能な少なくとも特定レベルのデータのアクセスを制御するため及び上記のユーザ入力装置を通してユーザの入力により上記の消去可能メモリ要素に記憶されたパスワード・データの変更を可能にするため、上記のユーザ入力装置と上記の消去可能メモリ要素に接続して動作するシステム・プロセッサと、

上記のカバー内に取り付けられ、パーソナル・コンピュータ・システムの動作のためのプログラムを記憶し、上記のシステム・プロセッサと接続して動作する読み取り専用メモリ（ＲＯＭ）装置と、

そのパーソナル・コンピュータ・システムが属しているネットワークを通してアクセス可能な複数の出所の中の選ばれた一つからオペレーティング・システムの初期導入を可能にするため、上記のＲＯＭ装置に記憶された優先づけた初期導入プログラムと、

そのパーソナル・コンピュータ・システムが属しているネットワークを通してアクセス可能で、そのパーソナル・コンピュータ・システムの通常のユーザと承認されていないユーザにはアクセスできないように、またシステム・オーナと承認されたユーザには、

（ａ）上記の複数の出所のグループの番号と優先順位を指定することによって上記の優先づけた初期導入プログラムを選択して変更し、

（ｂ）上記の入力装置を通して、ユーザの入力により上記の消去可能メモリ要素に記憶されたパスワード・データを選択して変更する、ようにプログラムされた機密保護ユーティリティ手段を備えるパーソナル・コンピュータ・システム。

【請求項２】　上記の消去可能メモリ要素が電気的に消去可能なプログラム可能読み取り専用メモリ装置である請求項１に記載のパーソナル・コンピュータ・システム。

【請求項３】　文字のユーザ入力のための鍵盤と、

通常閉じているカバーと、

カバー内に取り付けられ、パーソナル・コンピュータ・システムの動作中、プログラムの実行とデータの処理のため、鍵盤と接続して動作するシステム・プロセッサと、

上記のカバー内に取り付けられ、パーソナル・コンピュータ・システムの動作のためのプログラムを記憶し、上記のシステム・プロセッサと接続して動作する読み取り専用メモリ（ＲＯＭ）装置と、

複数の出所の中の選ばれた一つからオペレーティング・システムの初期導入を可能にするため、上記のＲＯＭ装置に記憶された優先づけた初期導入プログラムと、

パスワード・データを受け取り、記憶し、選択して動作可及び動作不可の状態にできるように上記のカバー内に取り付けられた消去可能なメモリ要素とを備えるＬＡＮステーション・パーソナル・コンピュータ・システムの機密保護機構の管理を容易にするための方法であって、

そのパーソナル・コンピュータ・システムが属しているネットワークを通してアクセス可能で、そのパーソナル・コンピュータ・システムの通常のユーザと承認されていないユーザにはアクセスできないように、またシステム・オーナと承認されたユーザには、上記の複数の出所のグループの番号と優先順位を指定することによって、上記の優先的初期導入プログラムを選択して変更することを可能にするために記憶された機密保護ユーティリティ・プログラムを使用し、それから、

そのパーソナル・コンピュータ・システムが属しているネットワークを通してアクセス可能で、そのパーソナル・コンピュータ・システムの通常のユーザと承認されていないユーザにはアクセスできないように、またシステム・オーナと承認されたユーザには、上記の入力装置を通して、ユーザの入力により上記の消去可能メモリ要素に記憶されたパスワード・データを選択して変更することを可能にするために記憶された機密保護ユーティリティ・プログラムを使用することを含む機密保護方法。

【発明の詳細な説明】

【０００１】この発明は１９９２年５月２７日付けで米国に出願し、この発明との関連出願である米国特許出願番号８８９，３２４及び８８９，３２５に記載されている発明と関連している。

【０００２】

【産業上の利用分野】この発明はパーソナル・コンピュータ・システム、特にワークステーションとしてローカル・エリア・ネットワークで使用され且つネットワーク内に保持され、また該システムで取扱い可能なデータのアクセス制御を可能にする機密保護機能を有するシステムと関連している。

【０００３】

【従来の技術】一般にパーソナル・コンピュータ・システム及び特にＩＢＭパーソナル・コンピュータは今日の近代社会における多くの分野にコンピュータ・パワーの利用を普及させた。パーソナル・コンピュータ・システムは通常次のように定義することが出きる。「単一のマイクロプロセッサと付随する揮発性又は不揮発性メモリを有する１つのシステムユニット、１つのデイスプレイ・モニタ、鍵盤、一つ又はそれ以上のディスケット装置、固定ディスク記憶装置及びオプションのプリンタによって構成される卓上型、床置き又は携帯用のマイクロコンピュータ」これらのシステムを他と区別する特徴の１つは上述の構成部分を互いに電気的に接続するためのマザーボード（システム・ボードとして知られており、また本明細書でも折りにふれてシステム・ボード、システム・プレーナ、プレーナと述べられている）を使用していることである。これらのシステムは主として個人ユーザ向けに独立した計算能力を提供するように設計されており、また個人や小規模ビジネスによる購買のため価格は低く設定されている。このようなパーソナル・コンピュータ・システムの例としてはIMB PERSONAL COMPUTER ATおよびIBM PERSONAL SYSTEM/2 モデル２５，３０，３５，４０，Ｌ４０ＳＸ，５０，５５，５６，５７，６５７０，８０，９０，９５がある。

【０００４】これらのシステムは２つの一般的系列に分類される。第１の系列は、これは通常系列１のモデルとして照会されているのであるが、IBM PERSONAL COMPUTER ATおよびその他「ＩＢＭ互換機」によって例証されるバス・アーキテクチャを使用している。第２の系列は、これは通常系列２のモデルとして照会されているのであるが、IBM PERSONAL SYSTEM/2 モデル５７から９５によって例証される、ＩＢＭのマイクロチャネル・バス・アーキテクチャを使用している。

【０００５】初期の系列 のモデルはシステム・プロセッサとして広く使われた ＩＮＴＥＬ８０８８又は８０８６マイクロプロセッサを典型的に使用した。その後の特定の系列１及び系列２のモデルは、低速のＩＮＴＥＬ８０８６マイクロプロセッサと類似の動作をさせるために実モード(Real Mode)で動作し或いはアドレス範囲をある種のモデルに対して１メガバイトから４ギガバイトへ拡張する保護モードで動作し得る高速のＩＮＴＥＬ８０２８６、８０３８６、及び８０４８６マイクロプロセッサを使用している。本質的に８０２８６、８０３８６及び８０３８６プロセッサの実モード機構は８０８６及び８０８８マイクロ・プロセッサ用に書かれたソフトウエアに対してハードウエアの互換性を提供している。

【０００６】ＩＢＭパーソナル・コンピュータのような最も初期のパーソナル・コンピュータから始まって、ソフトウエアの互換性は最重要事項として考えられてきた。この最終目標を達成するために、「ファームウエア」として知られるシステム・レジデント・コードの隔離層がハードウエアとソフトウエアの間に確立された。このファームウエアがユーザの適用業務プログラム／オペレーティング・システムと装置間のインターフェースを提供しハードウエア装置の諸特徴に係るわずらわしさからユーザを開放した。最終的には、該コードは基本入出力システム（ＢＩＯＳ）の中に組み込まれ、ハードウエアの特性から適用業務プログラムを隔離すると同時に新しい装置をシステムに追加することが許されるようになった。

【０００７】ＢＩＯＳが装置に対する中間インターフェースをデバイス・ドライバに提供すると同時にデバイス・ドライバをそれぞれのハードウエア装置の性質に依存する事から解放したためＢＩＯＳの重要性は、直ちに明白となった。ＢＯＩＳはシステム上不可欠な部分であり、システム・プロセッサに入出力されるデータの動きを制御するため、システム・プレーナ上に常駐し読みだし専用メモリ（ＲＯＭ）の形で客先へ出荷された。例えば、最初のＩＢＭパーソナル・コンピュータにおけるＢＩＯＳはプレーナ・ボード上のＲＯＭ ８Ｋを専有した。

【０００８】新しいパーソナル・コンピュータ系列が導入されるについて、ＢＩＯＳは新しいハードウエア及び入出力装置を包含するため更新したり、拡張しなければならなくなって来た。予期されたようにＢＩＯＳはメモリ容量を増加することから開始した。例えば、IBM PERSONAL COMPUTER AT 導入の際ＢＩＯＳは、３２Ｋバイトを必要とするに至った。

【０００９】今日、技術革新にともなって、系列２のパーソナル・コンピュータはさらに複雑になり、より頻繁に新モデルが消費者に提供されるようになりつつある。技術は急速に変化し、新しい入出力装置がパーソナル・コンピュータに追加されつつあるので、ＢＩＯＳの変更がパーソナル・コンピュータの開発過程で大きな問題となってきた。例えば、マイクロチャネル・アーキテクチャでのIBM PERSONAL SYSTEM/2の導入に際して、相当新しいＢＩＯＳ（新ＢＩＯＳ又はＡＢＩＯＳ）が開発された。しかしながら、ソフトウエアの互換性を保つために、系列１のモデルのＢＩＯＳが系列２のモデルに含まれなければならなかった。

【００１０】系列１のＢＩＯＳは後に互換ＢＯＩＳ又はＣＢＯＩＳとして知られるようになった。しかしながら、前にIBM PERSONAL COMPUTER ATに関して説明したとおり、わずか３２Ｋバイト ＲＯＭがプレーナ・ボードに有るだけであった。幸運にもシステムはＲＯＭを９６Ｋバイトに拡張することができた。不幸にしてこれが、ＢＩＯＳのために使用できる最大容量であることが判明した。そして更に幸運なことにＡＢＩＯＳを追加してもＡＢＩＯＳ、ＣＢＩＯＳ合わせて９６Ｋ ＲＯＭに縮小することができた。しかしながら、９６Ｋ ＲＯＭの中のほんの僅かな部分しか次の拡張のために残らなかった。将来、入出力装置を追加すれば結局はＣＢＩＯＳとＡＢＩＯＳはＲＯＭを使い果たしてしまうと考えられるようになった。かくして新しい入出力技術は簡単にはＣＢＩＯＳとＡＢＩＯＳの中に組み込めなくなるであろう。

【００１１】これらの問題のため、及び系列２のＢＩＯＳに対する変更を開発過程のできるだけ遅い時点で行いたいとする要請と相まって、ＲＯＭからＢＩＯＳの一部を取り去る必要性が生じてきた。これは、ＢＩＯＳの一部を固定ディスクのような大容量記憶装置に出来るだけディスク上のシステム区画として定義された部分に記憶させることによって達成された。該システム区画にはシステム・リファレンス・ディスケットのイメージを記憶させてあり、その中にはシステム構成を確立するための一種のユーティリティ・プログラム及び同等のプログラムが含まれている。

【００１２】ディスクには読みとり能力同様書き込み能力もあるのでＢＩＯＳの変更がディスク上で可能になった。ディスクはＢＩＯＳコードを迅速且つ効果的に記憶する手段を提供する一方、ＢＩＯＳコードが破壊される確率を著しく増加させた。ＢＩＯＳはオペレーティング・システムの不可欠の部分であるので破壊されたＢＩＯＳは異常な結果をもたらす可能性があり、多くの場合完全な動作不良及びシステムの不動作をもたらすことになる。かくして、正当と認められないＢＩＯＳのディスク上での変更を防止する手段が必要であることはきわめて明白になった。

【００１３】これが１９８９年８月２５日出願の米国特許出願番号０７／３９８，８２０、１９９１年６月４日発行の米国特許第５，０２２，０７７号の主題であった。興味ある読者は、ここに公開する発明の理解に役立つべき追加情報として該特許を参照されたい。そして該特許の内容は本発明の完全な理解のため必要な限り本明細書に参考として編入されている。

【００１４】ＩＢＭ ＰＳ／２マイクロチャネル・システムの導入の際、入出力アダプタ・ガード及びプレーナからスイッチやジャンパー線が取り除かれた。マイクロチャネル・アーキテクチャによってプログラム可能レジスタが提供され、これによってスイッチやジャンパー線が置き換えられたのである。これにともなって、これらプログラム可能レジスタ又はプログラム可能オプション選択（ＰＯＳ）レジスタを構成させるためのユーティリティが必要とされた。これらのユーティリティ及びその他システムの使用容易性を改良するためのユーティリティはシステム診断プログラムと共にシステム・リファレンス・ディスケットに組み込んで各システムに添付して出荷されるようになった。

【００１５】最初の使用に先立って、各マイクロチャネル・システムはそのＰＯＳレジスタを初期化する必要がある。例えば、もしそのシステムが新しい入出力カードを差し込み、或いはスロットを変更してシステム・プログラムの起動がなされると、構成エラーが生成表示され、システム起動手順は停止する。そこでユーザはシステム・リファレンス・ディスケットを差し込みＦ１キーを押すよう指示される。そこで「システム構成用ユーティリティ」がシステム構成のためシステム・リファレンス・ディスケットから起動される。システム構成用ユーティリティはユーザに必要な操作を指示する。

【００１６】もし適切な入出力の記述子ファイル（Descriptor File）がシステム・リファレンス・ディスケットに装頗されていれば、システム構成ユーティリティは正しいＰＯＳ又はシステム構成データを不揮発性メモリに生成する。記述子ファイルには該入出力カードをシステムとインターフェースさせるためのシステム構成情報が含まれている。

【００１７】近年における世界的パーソナル・コンピュータの普及と成長にともなって、ますます多くのデータや情報がこのようなシステムに収集され、保存され又は記録されるようになった。これらデータの中には本来機密を要するものも多い。悪用された場合、そのデータは人々を混乱に陥れ、会社は競争力を失い、或いは機密データは恐喝に使われ、或いは人々に対する物理的 力へ発展しかねない。多くのユーザがデータの機密性と価値を認識すればするほどますます係るデータの悪用を防止する必要がある。ユーザ自身及びそのデータと関連した人々を守るために、ユーザは購入するパーソナル・コンピュータにデータ保護、機密保護機能を必要としている。

【００１８】収集され、記録されたデータの機密保護の必要性を認識しているのはユーザだけではない。政府公共機関もまた法律を制定して機密データの保護を実施している。このような政府公共機関として米国政府がある。米国政府はかねてから事の重要性を認識し、それに答えてきた。米連邦政府は機密保護のレベルとそれぞれのレベルに対応する必要事項を定義し、証明機関を設けてパーソナル・コンピュータの製造業者にその製品を提出させ、その製品が各製造業者が主張している機密保護レベルに合致しているかどうか検査している。連邦政府による必要事項の原典は国防総省による「コンピュータ・システム信頼性評価基準（Trusted Computer System Evalnation Criteria) DOS ５２００．２８ ＳＴＤ－１９８２年１２月であり、一般に「オレンジ・ブック(Orange Book)」として知られている。米国政府は１９９２年１月１日に全ての政府関係データは、パーソナル・コンピュータ上では最低、機密保護レベルＣ－２で処理され、記録されなければならないと法制化した。

【００１９】コンピュータ・システム・ハードウエアに関しては、必要事項の本質は保証セクション、必要事項６に「高信頼機構は、いたずらや承認されていない変更

から恒常的に保護されなければならない．．．．」と記述されている。更に発展して、パーソナル・コンピュータは様々な方法により、様々なアーキテクチュアを通じて、ネットワークに組み込まれるようになった。ある特定のこれらのネットワークにおいては、パーソナル・コンピュータはメインフレームとして知られ、大規模データベースを提供し、データを扱う適用業務プログラムの存在場所としての強力なホスト・コンピュータと通信を行う「ダム(dumb)」端末機として主に使われている。

【００２０】一方別のネットワークでは、パーソナル・コンピュータが適用業務プログラムや、時にはデータを中央のファイル・サーバ（このファイル・サーバも大容量直接アクセス記憶装置を装備し、比較的迅速なデータの回復速度で動作可能なパーソナル・コンピュータである場合がある）から受取り、処理し、データ入力を受理し、且つファイル・サーバにデータを返送する「スマート（smart)」端末機として使われている。

【００２１】更にまた別のネットワーク構成に於いては、パーソナル・コンピュータ群がネットワーク内の１つ又は多数のシステムによって使用可能な資源群を共用している場合もある。これらの資源群としてはプリンタ、スキャナ、モデムなどの周辺機器や互いに資源を共有している１台のパーソナル・コンピュータに直接付属している各種直接アクセス記憶装置上の適用業務プログラム又はデータ・ファイルがある。これらネットワーク構成の多くは、ローカル・エリア・ネットワーク又はＬＡＮ（後者　ＬＡＮが本明細書上の限定用語である）として知られている。

【００２２】ＬＡＮに於けるパーソナル・コンピュータの使用が増大するにつれて、係る状況下で使用される１台あたりの機械の費用は、通常のパーソナル・コンピュータに見られるようなパーソナル・コンピュータの構成要素を取り除く事によって削減し得ると考えられるようになった。この結果、固定ディスクやフロッピー・ディスクのような直接アクセス記憶装置を持たないパーソナル・コンピュータが使用されるようになってきた。このようなシステムはメディアレス・システム或いはＬＡＮステーション（本明細書では、後者が限定用語となっている）として知られている。

【００２３】ローカル・エリア・ネットワークに於けるパーソナル・コンピュータの使用は、少なくともＢＩＯＳ機能としての部分に構成された特定の機能を持つような、いかなる典型的パーソナル・コンピュータに対しても、影響をもたらす原因になると考えられる。　これらの機能の中には（機密保護レベル　Ｃ－２を達成目標としている場合）いろいろな機密保護レベルの情報のアクセス管理が含まれるであろう。ＬＡＮに付随していない単体のパーソナル・コンピュータに関しては、自動構成機能が常識であり、一般に立ち上げ手順の一環として行われ、機密保護機構は最初に述べた関連出願（本発明の理解に必要な限り参考として本出願に編入されている）の機密保護機構を含む。

【００２４】ＬＡＮに付随したコンピュータに関しては、係る構成動作はコンピュータ内に組み込まれたＢＩＯＳの機能として動作し、立ちあげ手順の一環として処理される。しかしながら、ＬＡＮに接続されたコンピュータの構成動作は、当該コンピュータのパワーオン時点でＬＡＮによって自動的に行われる方が望ましい。　特に機密保護を必要とするＬＡＮに接続されたＬＡＮステーションの場合にはシステム・オーナ(System Owner)にとって、係るＬＡＮステーションからのＬＡＮに対する全ての攻撃への防御が至上命令となる。

【００２５】

【発明が解決しようとする課題】上述の議論を念頭に於いて、本発明はＬＡＮステーション・パーソナル・コンピュータ・システム（固定ディスク装置やフロッピー・ディスク装置のようなプログラム記憶媒体を持たない）であって承認されたユーザ又はシステム・オーナ（後述　定義のとうり）に対してＬＡＮ上でデータが安全にアクセス可能であるようなＬＡＮステーションを保証して提供する事を目的とする。

【００２６】

【課題を解決するための手段】ＬＡＮステーションは機密保護パスワードのような重大なデータのネットワーク上でのいかなる転送も回避する相当な手段を可能にする機密保護機構を必要とする場合がある。その代わりとしてＬＡＮステーションで承認されたユーザ又はシステム・オーナによって直接入力された係る重大データに関してシステムの安全を保証する手段又はシステム於ける対策がなされている。本発明の目的は、次の手段及び方法によって達成される。

【００２７】ネットワークとデータを交換し、システムにアクセス可能なデータを不正な（無許可の）アクセスから保護する能力を有するＬＡＮステーション・パーソナル・コンピュータ・システムであって、コマンドを入力するためのユーザ入力装置と、通常閉じているカバーと、カバー錠の鍵の所有者以外のカバー内部へのアクセスを拒絶するため、上記のカバーを機密保護状態に維持するためのカバー錠と、パスワード・データを受取り、記憶し、選択して動作可及び動作不可の状態にできるように上記のカバー内に取り付けられた消去可能なメモリ要素或いは電気的に消去可能でプログラム可能読み取り専用メモリ要素と、上記のカバーの内部に取り付けられ、カバーの中からのみアクセス可能で、上記の消去可能メモリ要素或いは電気的に消去可能でプログラム可能読み取り専用メモリ要素を動作可及び動作不可状態にセットするために上記の消去可能メモリ要素或いは電気的に消去可能でプログラム可能読み取り専用メモリ要素に接続して動作するオプション・スイッチと、上記のカバー内に取り付けられ、上記のメモリ要素の動作可及び動作不可状態を区別する事により、システムにアクセス可能な少なくとも特定レベルのデータのアクセスを制御するため及び上記のユーザ入力装置を通してユーザの入力により上記の消去可能メモリ要素或いは電気的に消去可能でプログラム可能読み取り専用メモリ要素に記憶されたパスワード・データの変更を可能にするため、上記のユーザ入力装置と上記の消去可能メモリ要素或いは電気的に消去可能でプログラム可能読み取り専用メモリ要素に接続して動作するシステム・プロセッサと、上記のカバー内に取り付けられ、パーソナル・コンピュータ・システムの動作のためのプログラムを記憶し、上記のシステム・プロセッサと接続して動作する読み取り専用メモリ（ＲＯＭ）装置と、そのパーソナル・コンピュータ・システムが属しているネットワークを通してアクセス可能な複数の出所の中の選ばれた一つからオペレーティング・システムの初期導入を可能にするため、上記のＲＯＭ装置に記憶された優先づけた初期導入プログラムと、そのパーソナル・コンピュータ・システムが属しているネットワークを通してアクセス可能で、そのパーソナル・コンピュータ・システムの通常のユーザと承認されていないユーザにはアクセスできないように、またシステム・オーナと承認されたユーザには、（ａ）上記の複数の出所のグループの番号と優先順位を指定することによって上記の優先づけた初期導入プログラムを選択して変更し、（ｂ）上記の入力装置を通して、ユーザの入力により上記の消去可能メモリ要素或いは電気的に消去可能でプログラム可能読み取り専用メモリ要素に記憶されたパスワード・データを選択して変更する．ようにプログラムされた機密保護ユーティリティ手段を備えるパーソナル・コンピュータ・システム。

【００２８】文字のユーザ入力のための鍵盤と、通常閉じているカバーと、カバー内に取り付けられ、パーソナル・コンピュータ・システムの動作中、プログラムの実行とデータの処理のため、鍵盤と接続して動作するシステム・プロセッサと、上記のカバー内に取り付けられ、パーソナル・コンピュータ・システムの動作のためのプログラムを記憶し、上記のシステム・プロセッサと接続して動作する読み取り専用メモリ（ＲＯＭ）装置と、複数の出所の中の選ばれた一つからオペレーティング・システムの初期導入を可能にするため、上記のＲＯＭ装置に記憶された優先づけた初期導入プログラムと、パスワード・データを受取り、記憶し、選択して動作可及び動作不可の状態にできるように上記のカバー内に取り付けられた消去可能なメモリ要素或いは電気的に消去可能でプログラム可能読み取り専用メモリ要素とを備えるＬＡＮステーション・パーソナル・コンピュータ・システムの機密保護機構の管理を容易にするための方法であって、そのパーソナル・コンピュータ・システムが属しているネットワークを通してアクセス可能で、そのパーソナル・コンピュータ・システムの通常のユーザと承認されていないユーザにはアクセスできないように、またシステム・オーナと承認されたユーザには、上記の複数の出所のグループの番号と優先順位を指定する事によって、上記の優先的初期導入プログラムを選択して変更することを可能にするために記憶された機密保護ユーティリティ・プログラムを使用し、それからそのパーソナル・コンピュータ・システムが属しているネットワークを通してアクセス可能で、そのパーソナル・コンピュータ・システムの通常のユーザと承認されていないユーザにはアクセスできないように、またシステム・オーナと承認されたユーザには、上記の入力装置を通して、ユーザの入力により上記の消去可能メモリ要素或いは電気的に消去可能でプログラム可能読み取り専用メモリ要素に記憶されたパスワード・データを選択して変更することを可能にするために記憶された機密保護ユーティリティ・プログラムを使用することを含む機密保護方法。

【００２９】

【実施例】これから本発明を添付図面を参照しながら詳細に説明するのであるが、図面では本発明の望ましい具体例が示されているのであり、通常の技術知識を有する人がここで述べる発明を修正しても、本発明の良好な結果が得られる。特定の限定用語が次のように使われている。

【００３０】トラステド・コンピューテイング・ベース(Trusted Computing Base)　ーＴＣＢ：コンピュータ・システム内に防御メカニズムが完備していること（ハードウェア、ファームウェア及びソフトウェアを含む）、実施する機密保護政策によりこれらを組み合わせる。ＴＣＢは１又は多数の要素で構成され、これら要素は共同して製品又はシステム上で統一した機密保護政策を実施する。機密保護政策を正確に実施するためのＴＣＢの能力は、もっぱらＴＣＢ内のメカニズムに依存し、またシステム運用員による機密保護関連のパラメータ(例えばユーザの認定）の正しい入力に依存する。

【００３１】トラステド・ソフトウェア（Trusted Software）：ＴＣＢのソフトウェア部分。

【００３２】トラステド・プログラム（Trusted Program）：トラステド・ソフトウェアに含まれるプログラム。

【００３３】オープン・プログラム（Open Program）：ＴＣＢ上で動作するプログラムでトラステド・プログラム以外のもの。

【００３４】リファレンス・モニタ・コンセプト（Reference Monitor Concept）：アクセス制御の概念で科目別対象に対する全てのアクセスを調停する概念機械を指す。

【００３５】セキュリテイ・カーネル（Security Kernel）：リファレンス・モニタ・コンセプトを実施するＴＣＢのハードウェア、ファームウェア、及びソフトウェアの要素。セキュリテイ・カーネルは全てのアクセスを調停し、変更されないように防御されており、且つ正しく

検証可能でなければならない。

【００３６】トラステド・コンピュータ・システム（Trusted Computer System）：一連の重要又は機密の情報を、同時に処理するために、その使用を許可されているハードウェア及びソフトウェアによる保全性を有するシステム。

【００３７】システム・オーナ（system Owner）：システム・オーナはシステムを最初に構成し、機密保護状態にする責任があるユーザのこと。システム・オーナは最初に且つ更新が必要な都度、その構成を管理する。システム・オーナは特権アクセス・パスワードを管理しその保全に責任を持つ。システム・オーナは不正アクセス防止用カバー錠の鍵について、その物理的保全性を維持する責任がある。システム・オーナはまた、全てのシステムの機密保護記録（log）を維持する責任がある。システム・オーナは試みられる全ての機密保護の侵害を記録しなければならない。システム・オーナは複数のシステムを受け持つ場合がある。システム・オーナは、承認されたユーザであり且つ通常のユーザでもあり得ると考えられる。

【００３８】機密保護モード（Secure Mode）：機密保護を構成する諸要素によって、機密防御機能を発動すべくシステム・オーナが特権アクセス・パスワードをパーソナル・コンピュータ上に正しく導入した状態。

【００３９】承認されたユーザ（Authorized User）：特権アクセス・パスワードを使用する事を承認せれた全てのユーザ。この人はシステム・オーナである場合もそうでない場合もある。この人はまた特定のシステム或いは複数システムをセットとして、鍵を保有する場合がある。もしこの人が機密保護に対する侵害からのシステム回復作業に関わる場合は、この人は責任を持って当該侵害の事実をシステム・オーナに報告しなければならない。承認されたユーザはまた通常のユーザである場合もある。

【００４０】通常のユーザ（Normal User）：システム設備を使用する事を承認された全てのシステム・ユーザ。システム構成を変更するため、又は発生した問題を解決するためには、このユーザはシステム・オーナか承認されたユーザの何れかの援助を必要とする。通常のユーザは承認されたユーザかシステム・オーナ部門の何れかに所属しない限り、特権アクセス・パスワードやカバー錠の鍵を持たない。

【００４１】承認されていないユーザ（Unautorized User）：システム・オーナ、承認されたユーザ又は通常のユーザの何れにも定義されていない人。承認されていないユーザによる機密保護を施したパーソナル・コンピュータの如何なる使用も、不成功に終わったパワーオンを除いて機密保護に対する侵害と考えられ、係る侵害を示す監査用追跡記録が存在しなければならない。

【００４２】ＥＥＰＲＯＭ：電気的に消去可能でプログラム可能な読み取り専用メモリ。このメモリ技術はハードウェアの論理回路によってデータの変更が可能な不揮発性メモリを提供する。パワーオフの状態でもメモリの内容は失われない。内容は、当該モジュールに適切な制御信号が事前に定義された手順で印加された場合にのみ変更される。

【００４３】パスワード記述（Password Description）：システムは次の２種類のパスワードによって保護される可能性を有する。１：特権アクセス・パスワード（Privileged Access Password - ＰＡＰ）。２：パワーオン・パスワード（Power On Password - ＰＯＰ）。これらパスワードは互いに独立して使用されるように意図されている。

【００４４】ＰＡＰはシステム・オーナに対して初期プログラム導入（ＩＰＬ）用装置起動リスト、パスワード・ユーテイリテイへのアクセス及びシステム・リファレンス・デイスケット・イメージへのアクセスを防止する事によって、防御を提供するように設計されている。

【００４５】本発明が関係するネットワーク環境に於いては、装置起動リスト、パスワード・ユーテイリテイ及びリファレンス・デイスケット又はシステム区画へのアクセスは、ＬＡＮステーションがメデイアレスであり、従って係るＬＡＮステーションでは直接アクセスの能力を欠いているために、ネットワーク・サーバを通じてのみ行われる。これが本発明の重要な特徴である。

【００４６】ＰＡＰの存在はＰＯＰを使用している通常のユーザとって明白である。ＰＡＰはサーバを通じてアクセス可能なシステム・リファレンス・デイスケット・イメージ上にあるユーテイリテイ・プログラムによって導入され、変更され、或いは削除される。ＰＡＰはもし正しく設定され、入力されれば、システム・オーナはＰＯＰに優先して、システム全体へのアクセスができることになる。

【００４７】ＰＯＰは、現在の全てのＰＳ／２で稼働しいるのであるが、ネットワーク・サーバ或いはネットワーク上の施設に対する如何なる不正なアクセスをも防止するために使用される。更に具体的に添付図面を参照すれば、本発明を具体化するマイクロコンピュータが１０（図１）に図示されている。上述の如く、コンピュータ１０はそれに付属したモニタ１１、鍵盤１２、プリンタまたはプロッタ１４を持っている。

【００４８】コンピュータ１０には図２に示したように、デイジタル・データを処理し、記憶するための電力によるデータ処理部及び記憶部を収容し、シャシ１９と共にこれらを包み、遮蔽するカバー１５がある。

【００４９】図２に示された形態において、コンピュータ１０には、コンピュータ・システムに関する入出力ケーブルの接続点を拡張し、併せて保護するオプションの入出力ケーブル接続用カバー１６がある。少なくともシステム構成部分のいくらかは、シャシ１９に固定された

多層プレーナ２０（ここではマザーボードまたはシステム・ボードとして記述されている）に収容されており、該多層プレーナは上述のコンピュータ構成部分や、その他付随するフロッピー・デイスク装置、各種の直接アクセス記憶装置、補助カード、ボード類を電気的に接続する手段を提供する。

【００５０】シャシ１９には、基盤と後部パネルがあり（図２、通常、ケーブル接続カバー１６によって外側から覆われている）、磁気或いは光学的デイスク装置、バックアップ用テープ装置類のようなデータ記憶装置を収容するための少なくとも一つの空間をとってある。

【００５１】図に示した形態において、上部空間２２は、第１サイズの周辺機器（３．５インチの装置として知られているもの）を収容するよう適合している。フロッピー・デイスク装置は、デイスケットを挿入し、そのデイスケットを使用してデータを受け取り、記録し、引き出す事ができる取り外し可能な媒体を使用した直接アクセス記憶装置として知られているが、通常該上部空間２２に収容される。

【００５２】しかしながら、ここで述べるＬＡＮステーションの場合には、システム１０の費用を削減するため、このような直接アクセス記憶装置は提供されない。本発明の上記構造について述べる前に、パーソナル・コンピュータ・システム１０の一般的動作についてその要点を再吟味する事は価値があるであろう。

【００５３】図３において、本発明によるシステム１０のようなコンピュータ・システムの各種構成部分を示すパーソナル・コンピュータのブロック・ダイアグラムが図示されている。このブロック・ダイアグラムには、プレーナ２０に収容された構成部分とプレーナと入出力スロット及びその他のパーソナル・コンピュータのハードウェアとの接続が含まれる。システム・プロセッサ３２もプレーナに接続されている。如何なるマイクロプロセッサでもＣＰＵ３２として使用して良いのであるが、一つの適切なマイクロプロセッサとしてインテル社から発売されている８０３８６がある。該ＣＰＵは、高速ＣＰＵバス３４によって、バス・インターフェース制御部３５、シングル・インライン・メモリ・モジュール（ＳＩＭＭｓ）として示される揮発性ランダム・アクセス・メモリ（ＲＡＭ）３６及びＣＰＵ３２に対する基本入出力動作の命令群を記憶するＢＩＯＳ　ＲＯＭ３８と接続されている。

【００５４】ＢＩＯＳ　ＲＯＭは、入出力装置とマイクロプロセッサ３２のオペレーテイング・システムとの間を整合させるために使用されるＢＩＯＳを含む。ＢＩＯＳＲＯＭ３８に記憶される命令群は、ＢＩＯＳの実行時間を減少させるためにＲＡＭ３６に複写する事ができる。

【００５５】当該システムはまた、すでに一般的になっているように、システム構成及び実時間クロック（ＲＴＣ）６８（図３）に関するデータを受信し、記憶する電池バックアップ型不揮発性メモリ（ＣＭＯＳ　ＲＡＭ及びＮＶＲＡＭとして知られている）を有する回路部を持つ。

【００５６】本発明は、今後図３のシステム・ブロック・ダイアグラムを特に参照しながら記述すのであるが、本発明による機械装置及び方法は、プレーナ・ボードの他のハードウェア構成でも使用され得る様に意図されている事を初めに理解されたい。例えば、当該システム・プロセッサはインテル社の８０２８６または８０４８６マイクロプロセッサでもかまわない。

【００５７】図３に帰って、ＣＰＵバス（bus）３４は（データ、アドレス、制御部を含む）またマイクロプロセッサ３２と数値演算用コプロセッサ（ＭＣＰＵ）３９との接続を行い、更に場合によっては、小型コンピュータ・システム・インターフェース（ＳＣＳＩ）制御部４０との接続も行う。もし存在していれば、ＳＣＳＩ制御部４０は、コンピュータの設計及び操作の分野の技術を有する人には自明のことではあるが、読みとり専用メモリ（ＲＯＭ）４１、ＲＡＭ４２、及び図の右側に表示された入出力接続端子によって容易となる各種の内部または外部装置と接続可能である。

【００５８】ＳＣＳＩ制御部４０は、固定または取り外し可能な媒体の電磁気的記憶装置（固定またはフロッピー・デイスク装置として知られている）、電気光学的、テープ及びその他の記憶装置を制御する記憶制御部として機能する。上述の通り、係る装置類は一般的に経済的理由によりＬＡＮステーション・パーソナル・コンピュータでは削除されており、同じ理由によりＳＣＳＩ制御部も削除される場合がある。しかしながら、ＬＡＮステーションの購入の際将来のシステムの格上げを意図する場合があるので、ＳＣＳＩ制御部のような要素或いはＤＡＳＤの為の空間などはしばしば用意されている。

【００５９】バス・インターフェース制御部（ＢＩＣ）３５は、ＣＰＵバス３４と入出力バス４４とを連結している。バス４４によって、ＢＩＣ３５は更に多くの入出力装置またはメモリ（図示されていない）を接続するためのマイクロチャネル・アダプタ・カード４５を収容するための複数の入出力スロットを有するマイクロチャネル・バスのようなオプション機構用バスと連結している。

【００６０】入出力バス４４はアドレス、データ、及び制御部をを含む。一般にＬＡＮステーション・システムに於いては、１枚のオプション・カード４５が当該システムとその属するネットワークとを接続する接続点を提供する。入出力バス４４と連結して、グラフィック情報（４８）や画像情報（４９）を記憶するビデオＲＡＭ（ＶＲＡＭ）に付随するビデオ信号処理部４６など各種の入出力部がある。

【００６１】プロセッサ４６で変換されたビデオ信号

は、デイジタル・アナログ変換器（ＤＡＣ）５０を通ってモニタまたはその他のデイスプレイ表示装置へ送られる。ここでは、ＶＳＰ４６を直接自然画像入出力と照会されている装置と接続する対応もなされている。これらの装置は、ビデオ・レコーダ／プレーヤ、カメラ等の形をとる場合がある。入出力バス４４はまた、デイジタル信号処理部（ＤＳＰ）５１と連結されており、そのＤＳＰ５１はＤＳＰ５１とその処理に関係したデータによる信号を処理するためのソフトウェア命令群を記憶する命令ＲＡＭ５２とデータＲＡＭ５４とを付随して持っている。ＤＳＰ５１は、音声制御部５５による音声入出力の処理とアナログ・インターフェース制御部５６によるその他の信号の処理を行う。

【００６２】最後に、入出力バス４４は入出力制御部５８及びそれに付随した電気的に消去可能でプログラム可能な読みとり専用メモリ（ＥＥＰＲＯＭ）５９と連結し、該ＥＥＰＲＯＭによって入力及び出力がフロッピー・デイスク装置、プリンタまたはプロッタ１４、鍵盤１２、マウスまたは指示器（図示されていない）、及びシリアル・ポートによる手段を含む一般周辺装置と交換される。ＥＥＰＲＯＭはここで述べる機密保護機能の一部を担当する。

【００６３】ここで述べるように、パーソナル・コンピュータ・システムの機密保護という特定の目的を達成するために、パーソナル・コンピュータ・システム１０は、その内部に選択して動作可能状態にしたり、動作不能状態にしたりでき、動作可能状態の時特権アクセス・パスワードを受け取って記憶するように、消去可能なメモリ要素を持っている。消去可能なメモリ要素は、電気的に消去可能でプログラム可能な読みとり専用メモリ又は上記ＥＥＰＲＯＭ５９（図３）の１フィールド又は部分であるここが望ましい。システムはまた、オプション又は機密保護スイッチをそのカバーを内部に設け、該メモリ要素の中の使用されたフィールド又は部分を動作可能又は動作不能状態にする為に、消去可能メモリ要素５９と接続して動作するようになっている。該オプション・スイッチ（本開示では機密保護スイッチとも呼ばれる）は、例えば、システム・プレーナ上のジャンパで、プレーナにアクセス可能な人によって、手作業で２種類の状態を設定できるものであっても良い。

【００６４】一つの状態（ここでは書き込み可能又はロック解除と呼ぶ）では、ＥＥＰＲＯＭ５９はここで述べるように動作可能状態に設定され、ＰＡＰを記憶できるようになっている。書き込み可能状態では、ＰＡＰはＥＥＰＲＯＭに書き込め、変更され、削除される。その他の或いは動作不能状態では、（ここでは、書き込み不可又はロック状態という）ＥＥＰＲＯＭのＰＡＰ記憶能力は、動作不能に設定されている。この発明によれば、ＬＡＮステーションの製造時の初期状態は、パワーオン時にシステムを機密不保護の状態に設定してある。

【００６５】システムが機密保護状態になるためには、システム・オーナは、施錠されたカバーを開けて、システム・プレーナ２０上にある機密保護スイッチの状態を意図的に変更し、機密保護パスワードの活性化を可能にし、システムを機密保護システムに成らしめなければならない。更に、システム・オーナ又は承認されたユーザは、手順を追って特別の処理を実行してＰＡＰの導入をしなければならない。係る処理とそれに適応するシステムの特徴が、本発明の焦点である。

【００６６】上述のように、システム１０はまた、図４の６８に示すように、消去可能なメモリ能力、すなはち電池による不揮発性ＣＭＯＳ　ＲＡＭ、及び実時間クロック（ＲＴＣ）を持つ第２の部分を有する。ＣＭＯＳ　ＲＡＭ又はＮＶＲＡＭは、本発明によれば、システム１０のパワーオン時にＰＡＰの成功的入力に関するデータを含むシステム構成を表示するデータを記憶する。少なくとも１個の不正な解錠の検出用スイッチ（図４、５、６）が用意され、カバー内に取り付けられ、カバーが開いている事を検出し、該不正な解錠検出用スイッチの動作に応答してメモリを消し去ったり或いはメモリ内に記憶されている特定のデータを設定したりするためのＣＭＯＳ　ＲＡＭと接続して動作するようになっている。

【００６７】システム・プロセッサ３２は、本発明によれば、ＥＥＰＲＯＭ５９とＣＭＯＳＲＡＭ６８に接続して動作し、メモリのＰＡＰ記憶能力の動作可又は動作不可の状態を区別し、正しいユーザすなはち記憶されている特権アクセス・パスワード（ＰＡＰ）による入力又は無入力を区別することによってシステム内に記憶された少なくとも特定のレベルのデータへのアクセスを一部制御するよう機能する。上記オプション・スイッチを操作する事によって、システム及びそれに関わるネットワークの操作員（具体的には、機密保護を維持し監督する立場にある人）は、ＥＥＰＲＯＭの状態を動作可或いは動作不可になるように選択してシステムを機密保護動作或いは機密保護でない動作になるよう選択する事ができる。もし機密保護動作が要請され実施する事になれば、システム・オーナはＰＡＰを入力しなければならない。

【００６８】ここで開示したように、この発明による機密保護業務に対応するシステムは、２つの別々の不揮発性で消去可能なメモリ要素、ＥＥＰＲＯＭ及びＣＭＯＳ　ＲＡＭを有する。この事は、本発明の時点で一部実施されたのであるが、ＰＡＰの状態の表示やＰＡＰの正しい入力は少なくとも無許可でカバーを開ける事の可能性と同様に、非常に多くの回数消去、書き込みの必要があるにも関わらずＥＥＰＲＯＭは、消去、書き込みサイクルの回数に関して寿命が限られているので、このようにした。このために、ここで述べる機能は、現在の技術に対応するため第１及び第２の消去可能なメモリ要素に分割されている。

【００６９】しかしながら、本発明は、これら２形態の

関連データは、もし技術が許すならば、或いはもし設計者が係る選択に伴う制限を受け入れるならば、単一の消去可能なメモリ要素に記憶させる事を意図している。

【００７０】ここで図４から図７までの概略図を参照する事によって、本発明に係る特定のハードウェア機構がより具体的に述べられている。図４は、一般的な電源制御又は「ＯＮ／ＯＦＦ」スイッチ６１、一般的電源６２、主カバー１５及びケーブル接続カバー１６の様なカバーの開放又は除去に応答して導通状態を変えるスイッチ、およびカバー錠スイッチ６４の特定の関係を示している。カバーの開放又は除去の状態を変えるスイッチは、本発明の図でいえば、２つある。すなはち、主カバー１５の除去に対して応答するスイッチ６５（図４、５、６）及びケーブル接続カバーの除去に応答するスイッチ６６である。

【００７１】各スイッチは２つの部分からなっている、１つは通常開（それぞれ６５ａ，６６ａ）、もう１つは通常閉（それぞれ６５ｂ，６６ｂ）である。第２のスイッチは、ケーブル接続カバー１６がそうであるように、オプションである。しかしながら、本明細書での注意深い考察によって明らかなように、オプション・カバーとスイッチは、システムに対するより完全な機密保護を保証する。

【００７２】通常開状態になっているカバー・スイッチ６５と６６の接点群は、主電源スイッチ６１と電源６２に直列に接続されている（図４）。従って、もしカバーをはずしてシステム１０の電源を入れようとすると、当該接点群６５ａと６６ａは開状態となりシステムの動作を防止する。カバーをしたままでると、当該接点群は閉じ状態になっているため、正常なシステム動作が開始され得る。

【００７３】通常閉状態のカバー・スイッチ６５と６６の接点群は、カバー錠スイッチ６４及びＣＭＯＳ　ＲＡＭ６８と直列に接続されている。当該通常閉状態の接点６５ｂと６６ｂは、カバー１５及び１６の存在によって開状態となり、これらカバーの除去によって閉状態となる。

【００７４】カバー錠スイッチ６４は、コンピュータ・システム１０に一般的に提供されているカバー錠を施錠する事によって、通常閉状態となる。これら３種類の接点群は、電流のグランドへの交代経路もしくはＣＭＯＳ　ＲＡＭの付勢化の一部分を形成しており、カバー錠が施錠状態になっているシステムの状態でカバーが不正に除去されたために、付勢化が失われれば、該メモリの特定区分を特定の状態（全て「１」で埋めるなど）に設定する効果を有する。

【００７５】当該メモリはＰＯＳＴ（Power On Self Test）によってチェックされているため、当該メモリ区分を特定の状態にする事は、構成エラー信号を発生し、システム・オーナに対して機密保護の侵害（成功か不成功かは別にして）が試みられた事を警報する事になる。

【００７６】メモリ区分を特定状態に設定するためには、オペレーテイング・システム起動のための事前に記憶されたパスワードが必要である。すなはち、本明細で別途開示したように、オペレーテイング・システムの起動には、正しいＰＡＰの入力が必要である。一般カバー錠スイッチ６４と主カバースイッチ６５は、主カバー上にある錠に関連して適切に位置ずけられるように、前面カード・ガイド部６９（図２、６）に取り付ける事が望ましい。前面カードガイド部は、コンピュータ・システム・フレーム上で、カバー１５が存在し、然るべき位置に置かれて、システムのカバーとして機能しているとき、カバースイッチ６５の発動レバー７０が、直立前面フレーム部の開口部に突き出るような位置に取り付けられている。

【００７７】ケーブル・カバースイッチ６６は、システム・フレームの後部パネルに取り付けられ、ケーブル・カバー１６上に取り付けられたラッチ部によって発動され且つ主カバー１５の場合と同様に手操作で鍵が回転できるように位置ずける事が望ましい。オプションのケーブル・カバー１６が使用されているとき、（完全なシステムの機密保護が必要な場合）、カバーを後部パネルに固定する事によって該、ラッチ部によって通常開の接点６６ａが閉状態になるように、また通常閉じの接点６６ｂが開状態になるように設定される。

【００７８】上述或いは後述の機密保護・保全機構は、前に提案されたパーソナル・コンピュータの機密保護機構、パワーオン・パスワード（ＰＯＰ）とは独立して動作する。係る追加の機密保護・保全機構は、オレンジ・ブックのような当面する規定のもとで、システム認定の為の安全な装置を提供する。

【００７９】もう一つのパスワードがシステムを機密保護状態にするために必要である。その新しいパスワードがここで言う特権アクセス・パスワード（ＰＡＰ）である。以前のパーソナル・コンピュータ・システムとの互換性を維持するために、ＰＯＰも依然として使用できるようになっている。

【００８０】パスワード保護はシステム・ハードウェア：ＥＥＰＲＯＭ、機密保護スイッチ及びカバー・スイッチ、ファームウェア、ＰＯＳＴ及びシステム・ソフトウェア・パスワード・ユーテイリテイ、によって実行される。一度ＰＡＰが導入されると、システムは機密保護モードになる。ＰＡＰはＥＥＰＲＯＭに保存される。ＰＡＰのバックアップ用コピーもＥＥＰＲＯＭに保存される。このKOTOは、ＰＡＰの導入、変更、削除の最中に電源断が発生して、ＰＡＰが偶発的に消失するのを防ぐために行われる。

【００８１】ＰＯＰ及びＰＡＰ（もし導入されていれば）の正当性を証明する少なくともいくつかの特定ビットがＮＶＲＡＭに記憶される。ＮＶＲＡＭ及びＥＥＰＲ

OMに保持されたデータの変更は互いに独立して行われる。ＥＥＰＲＯＭの中の２ビットが当該変更手順のどこで電源断が発生したかをＰＯＳＴに対して知らせ、できればシステム・ボードの交換の事態から再生させる機関として使われる。パスワード・ユーテイリテイは変更表示フィールド、ＰＡＰへアクセスする際に使われる２ビットの状態表示機関、を維持する。

【００８２】もしもパスワードの変更中に電源断が発生すれば、電源が再度回復した時ＰＯＳＴが上記状態表示機関をチェックする。（ＰＯＳＴは実際には、全てのパワーオン時点で該状態表示機関をチェックする。）もしＰＡＰの変更が成功すれば、（「００」状態）ＰＯＳＴは処理を続行する。もし変更が電源断の前に開始していれば、（「０１」状態）ＰＯＳＴは正当なバックアップＰＡＰの存在をチェックする。もし正当であれば、バックアップＰＡＰを主ＰＡＰへ複写する。もしオプション又は機密保護スイッチがロック解除の状態又は書き込み可能状態になっていなければエラーが表示される。この際システム・オーナは、カバーのロックを解除し、機密保護スイッチの位置を変えなければならない。

【００８３】もし主ＰＡＰの変更が成功すれば（「１０」状態）、システム・リファレンス・デイスケットの使用又はシステム区画の起動をしようとする試みを検証するために主ＰＡＰ（新ＰＡＰ）を使用する。ＰＯＳＴはバックアップＰＡＰが正しくないと想定し、この場合ＰＯＳＴは主ＰＡＰをバックアップＰＡＰに複写する。

【００８４】もしバックアップＰＡＰがうまく変更されていれば、（「１１」状態）主ＰＡＰ及びバックアップＰＡＰの両方とも正当であると考えられ、ＰＯＳＴはユーザによるＰＡＰの入力を確認する前に主ＰＡＰの正当性を検証する。上述のようにＰＯＰはＣＭＯＳメモリの中に維持されている。２ビットがＰＡＰの為のパスワード表示器として使用するためにＣＭＯＳメモリに維持されている。１つの表示器はシステムが機密保護モード（ＰＡＰが導入済み）にある事を示すために使用される。第２の表示器はＰＡＰが最初のパワーオン時（コールド・ブート - Cold Boot）には正しく導入されていた事を示すために使われる。

【００８５】これら２つの表示器は初期化されコールド・ブート時にのみ設定される。ＩＰＬに先立って、もしシステム・リファレンス・デイスケット又はシステム区画が起動されていなければ、これら表示器は書き込み保護され、該ＩＰＬは導入済みＰＡＰの入力が成功することを必要とする。ＰＯＰとこの表示器の変更はＥＥＰＲＯＭに記憶されたＰＡＰの変更と独立して行われる。しかしながら、ＣＭＯＳメモリの変更は、オペレーテイング・システムの導入を許し、回復のため正しいＰＡＰの入力が必要となる機密保護の侵害を表示することができる。

【００８６】パスワードに対する不正アクセスを防止するため、ＩＰＬ装置起動リスト、ＥＥＰＲＯＭ ＣＲＣ，及び全ての表示器は、オペレーテイング・システムを起動する初期プログラム導入（ＩＰＬ）に先立ってロックされる。係る分野を排除するため、ＰＯＳＴはシステムがパワーオフされない限りリセットされない特定のハードウェア・ラッチをセットする。

【００８７】ＰＯＳＴの第一段階（最初のパワーオン）のはじめに、ＰＯＳＴはＥＥＰＲＯＭがロックされているかどうかチェックする。もしロックされていれば、ＰＯＳＴはエラーを表示し、ハードウェアが機能していないとしてシステムを停止する。システム・オーナは、状況を矯正するため介入し、場合によってはシステム・ボードを取り替えなければならない。

【００８８】本発明の一形態に於いて、システムが物理的不正変更を加えられているとき、ＣＭＯＳ ＲＡＭの最初の１４バイトは影響を受けていない。次のＣＭＯＳ ＲＡＭの５０バイトは上で概説したように、全て「１」（バイナリ １）に設定される。この状況を検出したときＰＯＳＴは適当なエラー表示を行う。

【００８９】本発明のもう１つの形態に於いては、できるだけ小数のビット数がシステムの物理的不正変更表示として設定される。何れの例に於いても、システム・オーナ／承認されたユーザは、状況の矯正に介入しなければならず、その矯正にはシステム・リファレンス・デイスケット又はシステム区画起動のためパスワードを要請された時、ＰＡＰの入力が必要であったり、システム・ボードの取り替えが必要であったりする場合がある。もしシステム・オーナがＰＡＰを忘れたら、当該システム・ボードの取り替えが必要となろう。

【００９０】もしＰＯＰを忘れたら、システム・オーナは上述のようにＣＭＯＳ ＲＡＭの内容を捨てることができ、ＰＡＰ（もし導入されていれば）を入力してパスワード ユーテイリテイを実行するためにシステム・リファレンス・デイスケットを起動しＰＯＰを再導入することができる。

【００９１】何れのパスワードも未導入のままシステムがパワーオンされた時は、ＰＯＳＴはパスワードを要求するメッセージを出さない。しかしながら、ＰＯＳＴはＰＡＰ、バックアップ用ＰＡＰ、ＩＰＬ装置起動リスト及び全てのインヂケータをロックする。このことは、当該分野への如何なる偶発的或いは悪意のアクセスを防止するために行われる。

【００９２】システムがＰＯＰを導入し、ＰＡＰを導入しないままパワーオンされた時は、ＰＯＳＴはＰＯＰのチェックサム（Checksum）を検証する。もしチェックサムが合格であれば、ＰＯＳＴはユーザにＰＯＰの入力を要求する。もしチェックサムが不合格であれば、ＰＯＳＴはＣＭＯＳにあるＰＯＰを消去し、パスワードの入力を要求しない。

【００９３】ネットワーク上の如何なるプログラムの起動に先立って、ＰＡＰ，バックアップ用ＰＡＰ，ＩＰＬ装置起動リスト，ＥＥＰＲＯＭ ＣＲＣ及び全てのインヂケータはアクセスを防止するためロックされる。システムがＰＡＰを導入し、ＰＯＰを導入しないままパワーオンされた時は、ＰＯＳＴは状態表示機関の状況をチェックし、更にＰＡＰのパスワードのチェックサム（Checksum）を検証する。もしＰＡＰのチェックサムが合格であれば、ＰＯＳＴは通常の処理を続行する。もしＰＡＰのチェックサムが不合格であれば、エラー表示が行われシステムは停止する。

【００９４】この事は、ＰＯＳＴが偶発的にユーザに対して、ＥＥＰＲＯＭエラーのとき、以前に保護状態にあったシステムへの不保護状態でのアクセスを付与する状況を防止するために行われる。システム・オーナは、介入して状況の矯正をする必要があり、その矯正には場合によっては、システム・ボードの取り替えを要する。

【００９５】もしシステムが、正しいＰＡＰと正しいＰＯＰを導入した状態でパワーオンされていれば、ＰＯＳＴはユーザにパスワードの入力を促す。もしＰＯＰが入力されれば、ＰＯＳＴはシステム・リファレンス・デイスケット・イメージからの起動をしない。システムは現在のＩＰＬ装置リストのみを使用して起動する。

【００９６】もしＰＯＰでなくＰＡＰが入力されたら、該ユーザはシステム・リファレンス・デイスケット・イメージ（ネットワークに対するアクセスが可能であれば）、或いは正常なＩＰＬ装置リストから起動することができる。

【００９７】このパワーオン手順の後でシステム・リファレンス・デイスケット・イメージの起動がされるように、最初のパワーオン時にＰＡＰの入力が成功したことを知らせるインヂケータがセットされる。ＰＯＳＴは再起動のためにパスワードの入力を要求する事はない、従ってＰＡＰには、入力成功のインヂケータ及びその保護が必要である。ＰＯＳＴは、何れかのパスワードが正しく入力されたことを確認した後、確認のアイコンを表示することにより該入力を認証する。

【００９８】ＰＯＳＴの変更と連結して、パスワード・ユーテイリテイは、ＰＡＰに対するサポートを含まなければならない。該ユーテイリテイは、ＰＡＰの導入、変更、削除をサポートし、オプション・スイッチ或いは機密保護スイッチの位置とこれら３つの機能とは連動している。機密保護スイッチは承認されたユーザがＰＡＰのセットを行おうとするまでは、ロックの位置に止めて置くべきである。その時該ユーザは、システム・カバーを取り除き機密保護スイッチをロック解除（変更）の位置へ動かす必要がある。ここでＰＡＰがセットできるのである。機密保護スイッチがロック解除の位置になっているとき、ＥＥＰＲＯＭの外にあるハードウェア回路がＰＡＰをＥＥＰＲＯＭに書き込む事を許しいる。機密保護スイッチがロックの位置にあるとき、該ハードウェア回路は、ＰＡＰの場所に対する如何なる変更も防止している。機密保護スイッチがロックの位置にあるとき、承認されたユーザがＰＡＰを変更しようとすると、相当するメッセージが現れる。

【００９９】追加の安全機構がパスワード・ユーテイリテイに組み込まれていて、承認されたユーザがＰＡＰをＰＯＰと等しくセットする事を防止している。ＰＡＰをセットしたり変更するとき、該新ＰＡＰがシステムの現在のＰＯＰと等しくならないようにチェックがなされている。また、ＰＡＰを変更したり削除したりするときは、現在のＰＡＰを知っていなければならない。

【０１００】パーソナル・コンピュータ・システムは機密保護スイッチをロックの位置にし、カバーは施錠した状態で出荷されることになっている。このことは、システム・オーナ以外の如何なる人もシステムを機密保護モードにセットできないようにするために行われる。ＰＯＰと異なり、ＰＡＰはハードウェアの操作では消去されない。ＰＡＰを忘れたり、未詳認のユーザがシステムを機密保護モードにするには、システム・ボードを取り替えなければならない。

【０１０１】上述のメモリ要素、スイッチ、及びこれらの相互接続は、名前を付けた構成部分が特に機密保護機構を可能にするコンピュータ・システムの要素であることから、本明細書では「機密保護機構要素」として照会されている。

【０１０２】機密保護機構を有するＬＡＮステーションの通常の動作では、すでに述べたように、ＬＡＮステーションはパワーオンするとパワーオン・セルフテスト（ＰＯＷＥＲ ＯＮ ＳＥＬＦ ＴＥＳＴ ＝ ＰＯＳＴ）に入る。ＰＯＳＴ完了の直前にシステムは遠隔初期プログラム導入（ＲＩＰＬ）能力があることを検出する。ＲＩＰＬは通常オペレーテイング・システムがＬＡＮ上のサーバから供給されるようにしたもので、サーバはメデイアレス・ワークステーションに対する論理的プログラム起動装置として働く。ＰＯＳＴは係る装置からのＬＡＮステーション・プログラムの起動を実行する。ＰＯＳＴによって起動されるソフトウェアが未知であるため、ＰＯＳＴは機密保護機構装置内の全ての保護フィールドをロックする。

【０１０３】明白なように、ＬＡＮステーションをネットワーク上機密保護ワークステーションとするためには、ＰＡＰをセットする手段がなければならず、更にその手順がシステム・オーナや承認されたユーザにとって保護されなければならない。この結果を達成する事が本発明の焦点であり以後詳細に説明する。

【０１０４】ＰＡＰ或いはＩＰＬ装置起動リスト・フィールドを導入、変更又は削除するために、本発明により意図された１つの方法によれば、サーバとＬＡＮステーションの間に調整がなければならない。更に、ＬＡＮステーションのＮＶＲＡＭ６８の中に遠隔ＰＡＰ導入フラ

グの為の特別なフィールドを用意する必要がある。ＲＩＰＬの出所からシステム・リファレンス・デイスケット・イメージ或いは機器構成セット用ユーテイリテイの起動中、起動されるプログラムは、ＰＯＳＴによって指定された機密保護に関係するフィールドの状態を検出する。正常操作の結果として、上述のように、これらがロック状態である事が判ると、システム・リファレンス・デイスケット・プログラムは遠隔ＰＡＰ設定フラグをセットし、ＬＡＮステーションのパワーオフを行い、そして直ちに再びパワーオンするようにメッセージを発し、ＬＡＮステーションでのデータ処理を禁止する処置を取って終了する。

【０１０５】この時点でＬＡＮステーションでの承認されたユーザは、ステーションのパワーオフをし、またすぐにオンにする。ＰＯＳＴは、正常な動作を実行することによって、遠隔ＰＡＰ導入フラグの状態が変わったことを検出し、機密保護機構装置をロック解除にし、遠隔ＰＡＰ導入のためのフラグ・セットの変更やリセットを可能にしたまま、サーバからのプログラム起動の正常な動作を続行する。

【０１０６】サーバに定義されたＲＩＰＬの場所にはリファレンス・デイスケット・イメージ或いはシステム構成設定用プログラムが残っているため、そのプログラムが起動され、ＰＡＰを導入し、ＰＡＰを変更又は削除し、必要ならＩＰＬ装置起動リストの変更を行うことを可能にするにするために、承認されたユーザが、システム以前に機密保護装置の当該フィールドを変更できるようにする。

【０１０７】係る変更を完了するためには、承認されたユーザはシステムのパワーオフを再度行い、ＲＩＰＬに先立ってＰＯＳＴが機密保護装置フィールドのロックに戻れるようにメモリがクリアされている事を確認する必要がある。ＰＡＰをＬＡＮステーションに導入する第２の方法によれば、メデイアレス・ワークステーションに論理的プログラム導入装置を提供するサーバとワークステーションの間に同様に調整が必要である。しかしながら、この方法は、より短時間ですむため、ＥＥＰＲＯＭ及びＣＭＯＳに有る保護フィールドを上述の第１の方法より、短時間危険にさらすだけですむ。この方法は、メデイアレス・ステーションをパワーオフの状態でスタートさせる必要がある。

【０１０８】物理的にメデイアレス・ワークステーションの直近であれば、承認されたユーザは、上述の第１の方法のようにサーバのユーザに対して論理的起動装置をオペレーテイング・システム・イメージからシステム・リファレンス・デイスケット・イメージに変更するよう指示する。メデイアレス・ワークステーションの承認されたユーザは、それからワークステーションをパワーオンにする。承認されたユーザはこの時、ＰＯＳＴからの可視的表示を待って、鍵盤上で３つの連続打鍵、Ctrl-Alt-Ins、を行う。この連続打鍵は、ＰＯＳＴに対して、サーバの当該イメージを起動する前に、ＥＥＰＲＯＭとＣＭＯＳの保護フィールドが保護状態になっていない事を知らせるために使用される。

【０１０９】この状況に於いて、システム・リファレンス・デイスケット・イメージが起動され、ＰＡＰが導入され、或いはメデイアレス・ワークステーションの側から離れる前にシステムがパワーオフされている事を確認するのは、承認されたユーザの責任である。

【０１１０】ＰＯＳＴはビデオ・サブシステムを初期化し、テストとシステム内の他のサブシステムの初期化を行う。これは、メモリ、鍵盤、タイマ、及びＤＭＡ制御部を含む。鍵盤サブシステムが初期化されれば、承認されたユーザは該連続打鍵、Ctrl-alt-Ins、を行う事ができる。鍵盤サブシステムが初期化されれば、鍵盤ＢＩＯＳは、Ctrl-Alt-Ins、の打鍵を業界では有名になっている、Ctrl-Alt-Del.の識別と類似の方法で識別可能になる。この時承認されたユーザに対する可視的表示はなされていない。

【０１１１】ＰＯＳＴは鍵盤のＣＢＩＯＳをチェックして該打鍵が、鍵盤サブシステムの初期化とＰＯＳＴによって該打鍵入力のため、ウィンドウが開かれている事を知らせる可視的合図の送出との間に検出されたかどうか調べる。もし該打鍵がその間に検出されていたら、ＰＯＳＴはシステム区画起動打鍵検出ウィンドウを開かない。もし該打鍵がその間に検出されていなければ、ＰＯＳＴはシステム区画起動打鍵検出ウィンドウを開く。

【０１１２】ＰＯＳＴはそれから、デイスプレー上のカーソルを、現在位置、０行０列（上左隅）、から０行７９列（上右隅）へ動かす。これは、承認されたユーザにシステム区画起動打鍵検出ウィンドウが開かれている事を知らせるために行われる。次に、ＰＯＳＴはデイスケット・サブシステムを初期化し、アダプタをオンボード（on-board）ＲＯＭと共にシステムに統合するためにアダプタＲＯＭスキャンを行い、更にＳＣＳＩサブシステムの初期化を行う。

【０１１３】承認されたユーザが、起動手順中、保護フィールドを露出したままＰＯＳＴに知らせるため、該連続打鍵入力、Ctrl-Alt-Ins、をしなければならないのは、このウィンドウの間である。

【０１１４】この時点で、ＰＯＳＴはシステム区画起動打鍵検出ウィンドウを閉じ、デイスプレー上のビデオ・カーソルを０行７９列（右上隅）から初めの位置、０行０列（左上隅）へ戻す。この事がユーザに対してシステム区画起動打鍵検出ウィンドウが閉じられた事を示す事になる。もし承認されたユーザが、該連続打鍵を入力したとすれば、それが鍵盤の初期化後で、ウィンドウ開の前であっても、或いはウィンドウ開の間中であっても、ＰＯＳＴは、後の使用のため該打鍵の検出を表示するフラグをセットする。

【０１１５】もし承認されたユーザが、該打鍵入力の機会をのがしたら、その承認されたユーザは、最初に述べた方法に従ってＰＡＰを導入するか、この方法をやり直す事ができる。遠隔ＩＰＬに先行して、ＰＯＳＴは該打鍵フラグをチェックし、承認されたユーザがＥＥＰＲＯＭとＣＭＯＳの保護フィールドを不保護にして置く事を望んでいる事が判る。

【０１１６】ＰＯＳＴは正常な起動手順を、遠隔ＩＰＬの実行が必要であるという事を発見するまで進め、保護フィールド不保護の状態でその手順を進める。第１の方法の説明にあるように、起動イメージが装填されると、承認されたユーザはセット機構オプションを主メニュウの中から選択する。セット機構メニュウ上で承認されたユーザはパスワード・ユーテイリテイを発動するためセット・パスワードと不在開始モード(Unattended Start Mode)を選択する。承認されたユーザはそれから特権アクセス・パスワードを選択し、与えられた指示に従う。該ユーザは同時に、ＩＰＬ装置起動手順リストを定義し導入する必要がある。

【０１１７】これによって、承認されたユーザによって選択された起動装置が起動手順中いつも選択されている事が確認される。メデイアレス・ワークステーションを離れる前に、承認されたユーザはそのワークステーションのパワーオフをすべきである。さもなければ、もしそのワークステーションがパワーオンのままであると、ＥＥＰＲＯＭとＣＭＯＳの機密保護関係のフィールドが不正なアクセスの危険にさらされる。第１の方法の説明にあるように、この方法はＰＡＰの変更又は削除及びＩＰＬの装置起動手順リストの更新にも使用される。

【０１１８】ＰＯＳＴによってCtrl-Alt-Ins、の入力のために開かれたウィンドウは、米国特許出願で、１９９１年６月１７日出願の出願番号第７１６，５９４号に述べられている。

【０１１９】そこではそれがシステム・リファレンス・デイスケットを発動するために使用されている。本開示に於いては、それが遠隔ＩＰＬの為に保護フィールドがロック解除（open)になっている事をＰＯＳＴへ知らせるために使用されている。ＰＡＰの導入又は変更の処理が、ＰＡＰを定義している危険なデータの如何なるネットワーク上の転送も回避しており、それ故該データがネットワーク上に存在する可能性或いはネットワーク上で誤用される可能性を回避しているということが本発明にとって重要である。

【０１２０】図面と明細書に於いて本発明の望ましい具体化が説明され、特別の用語が使用されているけれども、説明は用語を一般的、記述的意識でのみ使用したのであり、制限を加える目的で使用したのではない。

【０１２１】

【発明の効果】本発明によれば、ＬＡＮステーション・パーソナル・コンピュータ・システム（固定デイスク装置やフロッピー・デイスク装置のようなプログラム記憶媒体を持たない）において、パスワード・データの如何なるネットワーク上の転送も回避し、それ故該データがネットワーク上に存在する可能性或いはネットワーク上で誤用される可能性を回避することができ、ＬＡＮ上での機密保護機能を提供することができる。

【図面の簡単な説明】

【図１】本発明を具体化する場合のパーソナル・コンピュータの外観図である。

【図２】図１のパーソナル・コンピュータの構成要素で、シャシ、カバー、プレーナ・ボードを含む分解部品配置図であり、これら構成要素の関係を示している。

【図３】図１及び図２のパーソナル・コンピュータの特定部分の概略図である。

【図４】図１及び図２のパーソナル・コンピュータの特定の構成部分で、本発明の機密保護に関連した部分を概略示したものである。

【図５】図１及び図２のパーソナル・コンピュータの特定の構成部分で、本発明の機密保護に関連した部分を概略示したものである。

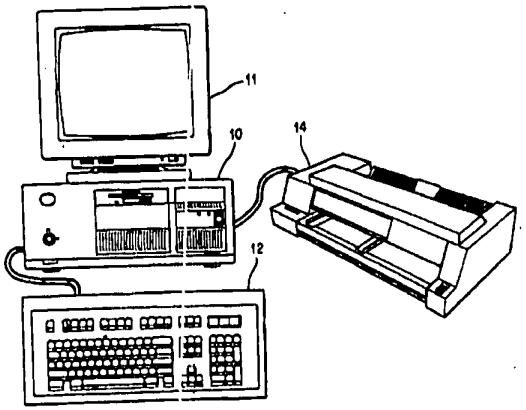
【図６】図４及び図５で表示された特定の構成部分の拡大外観図である。

【図７】本発明の機密保護機構に関連する図１、図２、図４及び図５で示されるパーソナル・コンピュータのオプション部分の拡大外観図である。

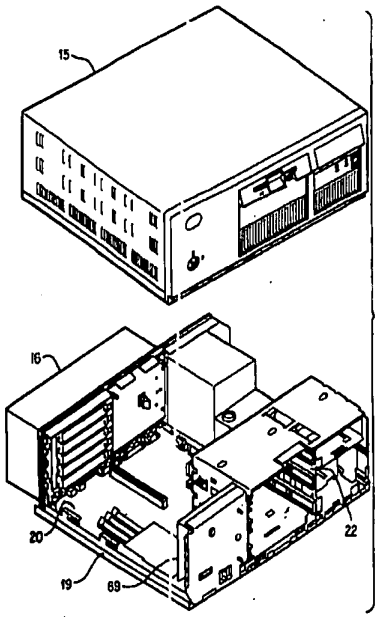
【符号の説明】

１０　パーソナル・コンピュータ
１１　デイスプレイ・モニタ
１２　鍵盤
１５　主カバー
１９　シャシ
２０　プレーナ・ボード
３６　ＳＩＭＭＳ（ＲＡＭ）
３８　ＢＩＯＳ　ＲＯＭ
５９　ＥＥＰＲＯＭ
６１　電源スイッチ
６２　電源
６４　カバー錠スイッチ
６８　ＲＴＣ／ＣＭＯＳ　ＲＡＭ

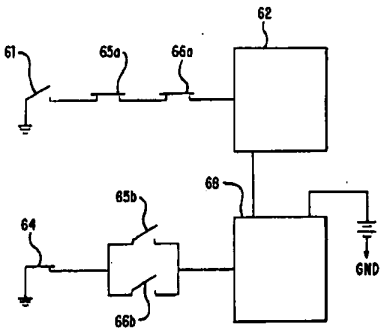
【図1】


11
10
14
12

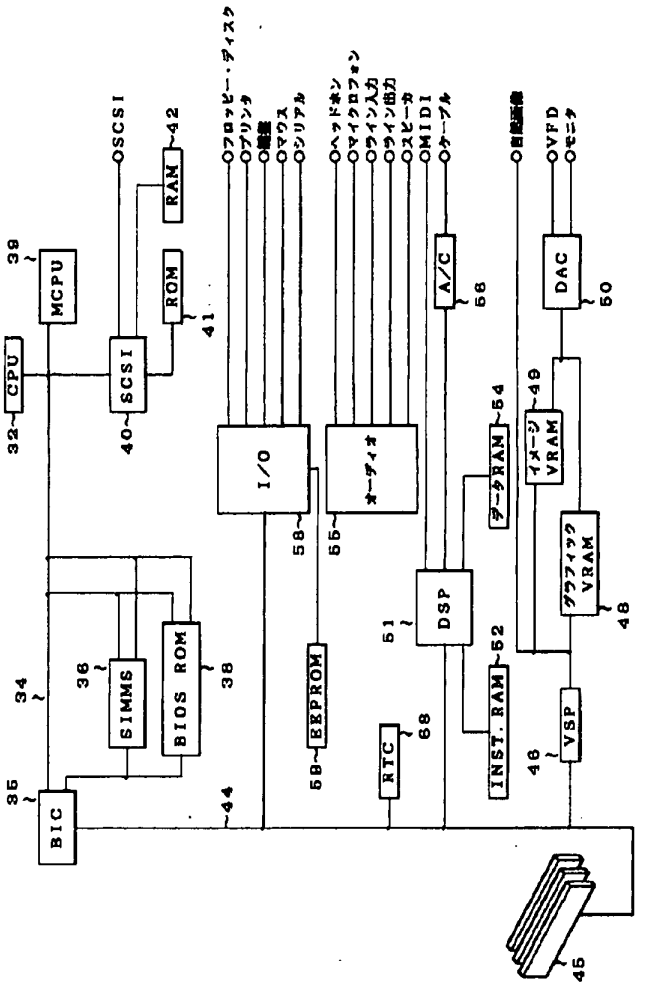
【図2】


15
16
20
22
19
69

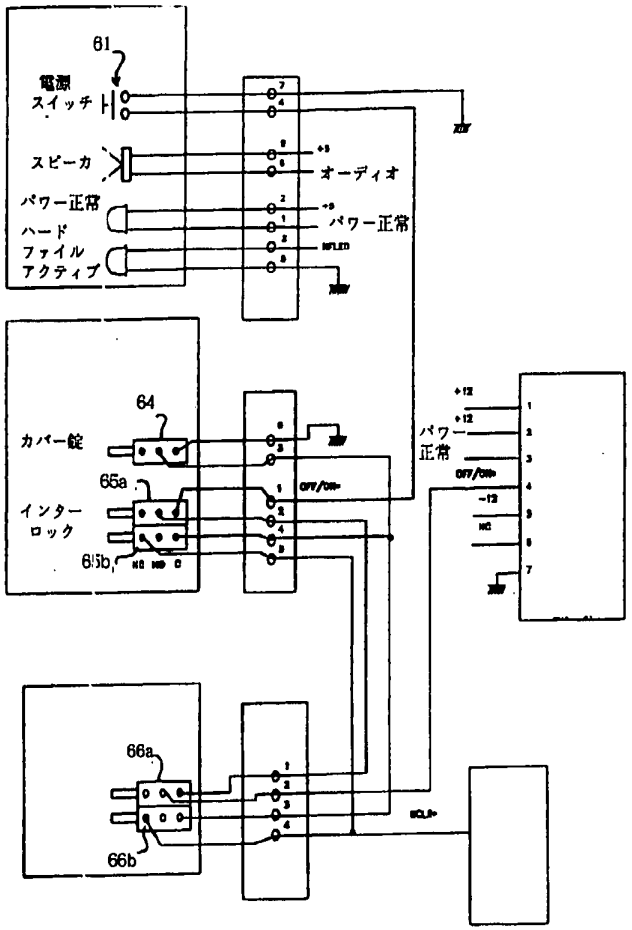
【図4】


62
61
65a
66a
68
65b
64
GND
66b

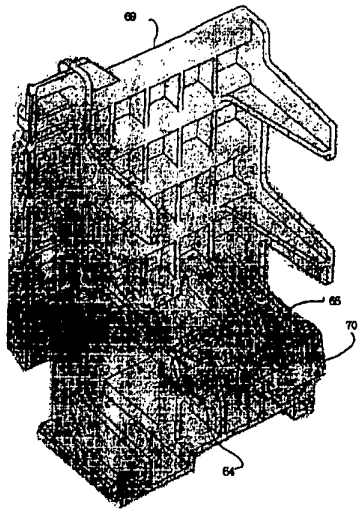
【図3】


MCPU
39
CPU
32
SCSI
40
RAM
42
ROM
41
フロッピー・ディスク
プリンタ
HDD
マウス
シリアル
SCSI
I/O
58
ヘッドホン
マイクロフォン
ライン入力
ライン出力
スピーカ
MIDI
ケーブル
オーディオ
55
A/C
56
DAC
50
VFD
モニタ
イメージ
VRAM
49
データRAM
54
グラフィック
VRAM
48
DSP
51
INST. RAM
52
VSP
46
RTC
68
EEPROM
58
SIMMS
36
BIOS ROM
38
34
BIC
35
44
45

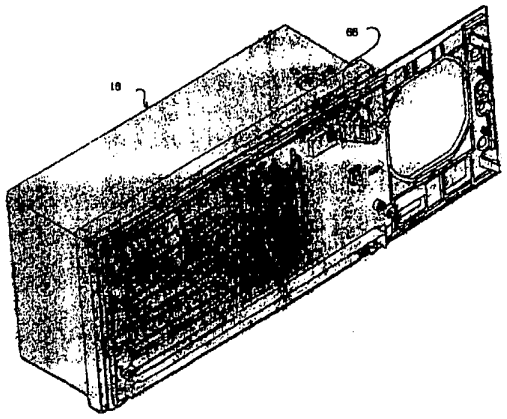
【図５】



【図６】



【図７】



フロントページの続き

(72)発明者　キムサン・ド・レ
アメリカ合衆国　33437　フロリダ州・ボイントン・ビーチ　サン・ポイント・ドライブ　9422

(72)発明者　マッシュウ・テイー・ミッテルステッド
アメリカ合衆国　30144　ジョウジア州・ケネソウサンダーリングス・ポイント　3550

(72)発明者 バーマー・イー・ニューマン
アメリカ合衆国 33433 フロリダ州・ボカラトンダブリン・ドライブ 7488
(72)発明者 デーブ・リー・ランドール
アメリカ合衆国 33068 フロリダ州・ポンパノ・ビーチ 69テラス 1751 エス・ダブリュウ
(72)発明者 リサ・アンネ・ルオトロ
アメリカ合衆国 33467 フロリダ州・レイク・ワース アウアチタ・ドライブ 5264
(72)発明者 ジョアンナ・バーガー・ヨダ
アメリカ合衆国 27513 ノースカロライナ州・ケアリー カスター・トレイル 203